I

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

EMERALD 1997 invalidates the indicated claims under 35 U.S.C. § 102(b) and 35 U.S.C. § 103*

All text citations are taken from: P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", 20th NISSC October 9, 1997 [SYM_P_0068831- SYM_P_0068843]. SRI admits this paper was published on Oct. 9, 1997 in the Proceedings of the 20th National Information Systems Security Conference. *See* SRI Response to ISS's First Set of RFAs, #1.

The text included herein are merely representative samples of the disclosure in the asserted reference. I reserve the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- P. Neumann, P. Porras and A. Valdes, "Analysis and Response for Intrusion Detection in Large Networks," Summary for CMAD Workshop, Monterey, 12-14 November 1996. [SYM_P_0499439- SYM_P_0499440].
- "Analysis and Response for Intrusion Detection in Large Networks," Summary for CMAD Workshop, Monterey, 12-14 November 1996 [SRI011022-SRI011026].
- "Analysis and Response for Intrusion Detection in Large Networks," Summary for Intrusion Detection Workshop, Santa Cruz, 26-28 August 1996 [SRI011045-SRI011048].
- P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances Conceptual Overview," December 18, 1996. [SYM_P_0503335- SYM_P_0503345].
- P. Porras and P. Neumann, "CONCEPTUAL DESIGN AND PLANNING for EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Version 1.2 May 20, 1997, http://www.csl.sri.com/intrusion.html [SRI012308-SRI012404].

* 103 references are identified under the heading "**103:**".

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
1	A method of network surveillance, comprising:	*"The EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) environment is a distributed scalable tool suite for tracking malicious activity through and across large networks. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. It combines models from research in distributed high-volume event-correlation methodologies with over a decade of intrusion detection research and engineering experience. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network. These monitors contribute to a streamlined event-analysis system that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services on the Internet."* p. 353 [SYM_P_006883] "The typical target environment of the EMERALD project is a large enterprise network with thousands of users connected in a federation of independent administrative *domains*. Each administrative domain is viewed as a collection of local and network services that provide an interface for requests from individuals internal and external to the domain. p. 354 [SYM_P_0068832] "EMERALD introduces a hierarchically layered approach to network surveillance that includes *service analysis* covering the misuse of individual components and network services within the boundary of a single domain; *domain-wide analysis* covering misuse visible across multiple services and components; and *enterprise-wide analysis* covering coordinated misuse across multiple domains." p. 355 [SYM_P_0068833]
	receiving network packets handled by a network entity;	"Event Generation and Storage: Audit generation and storage has tended to be a centralized activity, and often gathers excessive amounts of information at inappropriate layers of abstraction. Centralized audit mechanisms place a heavy burden on the CPU and I/O throughput, and simply do not scale well with large user populations. In addition, it is difficult to extend centralized audit

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances
"EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		mechanisms to cover spatially distributed components such as network infrastructure (e.g., routers, filters, DNS, firewalls) or various common network services." p. 354 [SYM_P_0068832] "Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering." p. 355 [SYM_P_0068833] "The generic EMERALD monitor architecture is illustrated in Figure 1. The architecture is designed to enable the flexible introduction and deletion of analysis engines from the monitor boundary as necessary. In its dual-analysis configuration, an EMERALD monitor instantiation combines signature analysis with statistical profiling to provide complementary forms of analysis over the operation of network services and infrastructure. In general, a monitor may include additional analysis engines that may implement other forms of event analysis, or a monitor may consist of only a single resolver implementing a response policy based on intrusion summaries produced by other EMERALD monitors. Monitors also incorporate a versatile application programmers' interface that enhances their ability to interoperate with the analysis target, and with other third-party intrusion-detection tools. Underlying the deployment of an EMERALD monitor is the selection of a target-specific event stream. The event stream may be derived from a variety of sources including audit data, network datagrams, SNMP traffic, application logs, and analysis results from other intrusion-detection instrumentation. The event stream is parsed, filtered, and formatted by the target-specific event-collection methods provided within the resource object definition (see Section III-B). Event records are then forwarded to the monitor's analysis engine(s) for processing. EMERALD's *profiler engine* performs statistical profile-based anomaly detection given a generalized event stream of an analysis target (Section III-C). EMERALD's *signature engine* requires minimal state-management and employs a rule-coding scheme that breaks from traditional expert-system techniques to provide a more focused and distributed signature-analysis model (Section III-D). Multiple analysis engines implementing different analysis methods may be employed to analyze a variety of event streams that pertain to the same analysis target."

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances
"EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		p. 356 [SYM_P_0068834] "Similarly, the analysis engines are responsible for establishing and maintaining a communication link with a target event collection method (or event filter) and prompting the reconfiguration of the collection method's filtering semantics when necessary. Event collection methods provide analysis engines with target-specific event records upon which the statistical and signature analyses are performed." p. 362 [SYM_P_0068840] "EMERALD also provides a framework for recognizing more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an entire network enterprise. … It generalizes to network environments the Safeguard experience [2], which overcame profile explosion and scalability problems by locally profiling the activities of subsystems and commands rather than of individual users." p. 364 [SYM_P_0068842] "EMERALD also extends the statistical-profile model of NIDES, to analyze the operation of network services, network infrastructure, and activity reports from other EMERALD monitors. Various other efforts have considered one of the two types of analysis - signature-based (e.g., Porras [18] has used a state-transition approach; the U.C. Davis and Trident DIDS [4] addresses abstracted analysis for networking, but not scalability; the Network Security Monitor [7] seeks to analyze packet data rather than conventional audit trails; Purdue [5] seeks to use adaptive-agent technology) or profile-based. More recent work in UC Davis' GrIDS effort [24] employs *activity graphs* of network operations to search for traffic patterns that may indicate network-wide coordinated attacks." p. 364 [SYM_P_0068842]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances
"EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
	building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets	"EMERALD's *profiler engine* performs statistical profile-based anomaly detection given a generalized event stream of an analysis target (Section III-C)." p. 356 [SYM_P_0068834] "Requirements for an anomaly-detection system that became IDES were documented in [6]. This research led to the development of the NIDES statistical profile-based anomaly-detection subsystem (NIDES/Stats), which employed a wide range of multivariate statistical measures to profile the behavior of individual users [9]. Analysis is user-based, where a statistical score is assigned to each user's session representing how closely currently observed usage corresponds to the established patterns of usage for that individual. The input source to the NIDES statistical component is an unfiltered and unsorted host audit log, which represents the activity of all users currently operating on the host. In 1995, SRI conducted research under Trusted Information Systems' Safeguard project to extend NIDES/Stats to profile the behavior of individual applications [2]. Statistical measures were customized to measure and differentiate the proper operation of an application from operation that may indicate Trojan horse substitution. Under the Safeguard model, analysis is application-based, where a statistical score is assigned to the operation of applications and represents the degree to which current behavior of the application corresponds to its established patterns of operation. The Safeguard effort demonstrated the ability of statistical profiling tools to clearly differentiate the scope of execution among general-purpose applications. While NIDES/Stats has been reasonably successful profiling users and later applications, it will be extended to the more general subject class typography required by EMERALD. Nonetheless, the underlying mechanisms are well suited to the problem of network anomaly detection, with some adaptation. The required modifications center around extensive reworking of NIDES/Stats to abstract and generalize its definition of measures and profiles, the streamlining of its profile management, and the adaptation of the configuration and reporting mechanisms to EMERALD's highly interoperable and dynamic message system interface. The EMERALD profiler engine achieves total separation between profile management and the mathematical algorithms used to assess the anomaly of events. Profiles are provided to the computational engine as classes defined in the resource object. The mathematical functions for anomaly scoring, profile maintenance, and updating function in a fully general manner, not requiring any underlying knowledge of the data being analyzed beyond what is encoded in the profile class. The event-collection interoperability supports translation of elementary data (the analysis target's event stream) to the profile and measure classes. At that point, analysis

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		for different types of monitored entities is mathematically similar. This approach imparts great flexibility to the analysis in that fading memory constants, update frequency, measure type, and so on are tailored to the entity being monitored. Each profiler engine is dedicated to a specific target event stream at the elementary level. Such localized, target-specific analyses (unlike the monolithic approach employed by NIDES/Stats) provide a more distributed, building-block approach to monitoring, and allow profiling computations to be efficiently dispersed throughout the network. Because the event stream submitted to the profiler engine is specific to the analysis target's activity, profile management is greatly simplified, in that there is no need to support multisubject profile instantiations. In addition, the results of service-layer profiler engines can be propagated to other monitors operating higher in EMERALD's layered analysis scheme, offering domain- or enterprise-wide statistical profiling of anomaly reports. Profiler engines may operate throughout the analysis hierarchy, further correlating and merging service-layer profiles to identify more widespread anomalous activity. The underlying mathematics are the same for each instance, and all required information specific to the entity being monitored (be it a network resource or other EMERALD monitors producing analysis results at lower layers in the analysis hierarchy) is entirely encapsulated in the objects of the profile class." p. 359 [SYM_P_0068837] "The basic analysis unit in this architecture is the EMERALD monitor, which incorporates both signature analysis and statistical profiling. By separating the analysis semantics from the analysis and response logic, EMERALD monitors can be easily integrated throughout EMERALD's layered network surveillance strategy." p. 364 [SYM_P_0068842] **103:** A. Valdes and D. Anderson, *Statistical Methods for Computer Usage Anomaly Detection Using NIDES*, Proc. of the Third International Workshop on Rough Sets and Soft Computing, January 1995 ("*Statistical Methods*") [SYM_P_0068937-942].

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
	the at least one measure monitoring data transfers, errors, or network connections;	"Event Generation and Storage: Audit generation and storage has tended to be a centralized activity, and often gathers excessive amounts of information at inappropriate layers of abstraction. Centralized audit mechanisms place a heavy burden on the CPU and I/O throughput, and simply do not scale well with large user populations. In addition, it is difficult to extend centralized audit mechanisms to cover spatially distributed components such as network infrastructure (e.g., routers, filters, DNS, firewalls) or various common network services." p. 354 [SYM_P_0068832] "Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering." p. 355 [SYM_P_0068833] "Underlying the deployment of an EMERALD monitor is the selection of a target-specific event stream. The event stream may be derived from a variety of sources including audit data, network datagrams, SNMP traffic, application logs, and analysis results from other intrusion-detection instrumentation. The event stream is parsed, filtered, and formatted by the target-specific event-collection methods provided within the resource object definition (see Section III-B). Event records are then forwarded to the monitor's analysis engine(s) for processing. EMERALD's *profiler engine* performs statistical profile-based anomaly detection given a generalized event stream of an analysis target (Section III-C). EMERALD's *signature engine* requires minimal state-management and employs a rule-coding scheme that breaks from traditional expert-system techniques to provide a more focused and distributed signature-analysis model (Section III-D). Multiple analysis engines implementing different analysis methods may be employed to analyze a variety of event streams that pertain to the same analysis target." p. 356 [SYM_P_0068834] "Similarly, the analysis engines are responsible for establishing and maintaining a communication link with a target event collection method (or event filter) and prompting the reconfiguration of the collection method's filtering semantics when necessary. Event

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances
"EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		collection methods provide analysis engines with target-specific event records upon which the statistical and signature analyses are performed." p. 362 [SYM_P_0068840] "EMERALD also provides a framework for recognizing more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an entire network enterprise. … It generalizes to network environments the Safeguard experience [2], which overcame profile explosion and scalability problems by locally profiling the activities of subsystems and commands rather than of individual users." p. 364 [SYM_P_0068842] "EMERALD also extends the statistical-profile model of NIDES, to analyze the operation of network services, network infrastructure, and activity reports from other EMERALD monitors. Various other efforts have considered one of the two types of analysis - signature-based (e.g., Porras [18] has used a state-transition approach; the U.C. Davis and Trident DIDS [4] addresses abstracted analysis for networking, but not scalability; the Network Security Monitor [7] seeks to analyze packet data rather than conventional audit trails; Purdue [5] seeks to use adaptive-agent technology) or profile-based. More recent work in UC Davis' GrIDS effort [24] employs *activity graphs* of network operations to search for traffic patterns that may indicate network-wide coordinated attacks." p. 364 [SYM_P_0068842] *See also* associated discussion in my expert report.
	comparing at least one long-term and at least one short-term statistical profile; and	"EMERALD's *profiler engine* performs statistical profile-based anomaly detection given a generalized event stream of an analysis target (Section III-C)." p. 356 SYM_P_0068834] "Requirements for an anomaly-detection system that became IDES were documented in [6]. This research led to the development of

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		the NIDES statistical profile-based anomaly-detection subsystem (NIDES/Stats), which employed a wide range of multivariate statistical measures to profile the behavior of individual users [9]. Analysis is user-based, where a statistical score is assigned to each user's session representing how closely currently observed usage corresponds to the established patterns of usage for that individual. The input source to the NIDES statistical component is an unfiltered and unsorted host audit log, which represents the activity of all users currently operating on the host. In 1995, SRI conducted research under Trusted Information Systems' Safeguard project to extend NIDES/Stats to profile the behavior of individual applications [2]. Statistical measures were customized to measure and differentiate the proper operation of an application from operation that may indicate Trojan horse substitution. Under the Safeguard model, analysis is application-based, where a statistical score is assigned to the operation of applications and represents the degree to which current behavior of the application corresponds to its established patterns of operation. The Safeguard effort demonstrated the ability of statistical profiling tools to clearly differentiate the scope of execution among general-purpose applications. While NIDES/Stats has been reasonably successful profiling users and later applications, it will be extended to the more general subject class typography required by EMERALD. Nonetheless, the underlying mechanisms are well suited to the problem of network anomaly detection, with some adaptation. The required modifications center around extensive reworking of NIDES/Stats to abstract and generalize its definition of measures and profiles, the streamlining of its profile management, and the adaptation of the configuration and reporting mechanisms to EMERALD's highly interoperable and dynamic message system interface. The EMERALD profiler engine achieves total separation between profile management and the mathematical algorithms used to assess the anomaly of events. Profiles are provided to the computational engine as classes defined in the resource object. The mathematical functions for anomaly scoring, profile maintenance, and updating function in a fully general manner, not requiring any underlying knowledge of the data being analyzed beyond what is encoded in the profile class. The event-collection interoperability supports translation of elementary data (the analysis target's event stream) to the profile and measure classes. At that point, analysis for different types of monitored entities is mathematically similar. This approach imparts great flexibility to the analysis in that fading memory constants, update frequency, measure type, and so on are tailored to the entity being monitored. Each profiler engine is dedicated to a specific target event stream at the elementary level. Such localized, target-specific analyses (unlike the monolithic approach employed by NIDES/Stats) provide a more distributed, building-block approach to monitoring, and allow profiling computations to be efficiently dispersed throughout the network. Because the event stream submitted to the profiler

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		engine is specific to the analysis target's activity, profile management is greatly simplified, in that there is no need to support multisubject profile instantiations. In addition, the results of service-layer profiler engines can be propagated to other monitors operating higher in EMERALD's layered analysis scheme, offering domain- or enterprise-wide statistical profiling of anomaly reports. Profiler engines may operate throughout the analysis hierarchy, further correlating and merging service-layer profiles to identify more widespread anomalous activity. The underlying mathematics are the same for each instance, and all required information specific to the entity being monitored (be it a network resource or other EMERALD monitors producing analysis results at lower layers in the analysis hierarchy) is entirely encapsulated in the objects of the profile class." p. 359 [SYM_P_0068837] **103:** A. Valdes and D. Anderson, *Statistical Methods for Computer Usage Anomaly Detection Using NIDES*, Proc. of the Third International Workshop on Rough Sets and Soft Computing, January 1995 ("*Statistical Methods*") [SYM_P_0068937-942].
	determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.	"Multiple analysis engines implementing different analysis methods may be employed to analyze a variety of event streams that pertain to the same analysis target. These analysis engines are intended to develop significantly lower volumes of abstract *intrusion* or *suspicion reports*. The profiler and signature engines receive large volumes of event logs specific to the analysis target, and produce smaller volumes of intrusion or suspicion reports that are then fed to their associated *resolver*." p. 356 [SYM_P_0068834] **103:** A. Valdes and D. Anderson, *Statistical Methods for Computer Usage Anomaly Detection Using NIDES*, Proc. of the Third International Workshop on Rough Sets and Soft Computing, January 1995 ("*Statistical Methods*") [SYM_P_0068937-942].

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
2	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer commands	See '338 claim 1 and associated discussion in my expert report. **103:** NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-79 to 4-80 [SYM_P_0075135-36]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A. NFR. *See* Ranum et al., "Implementing a Generalized Tool for Network Monitoring," Proceedings of the Eleventh Systems Administration Conference (LISA '97), San Diego, CA, Oct. 1997 [SYM_P_0070720-28], 5-6 [SYM_P_0070725-26].
3	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer errors.	See '338 claim 1 and associated discussion in my expert report. **103:** NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-79 - 4-80 [SYM_P_0075135-36], 4-61 [SYM_P_0075117], 4-67 [SYM_P_0075123], 4-69 [SYM_P_0075125], 4-82 [SYM_P_0075138]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A.
4	The method of claim 1, wherein the measure monitors data transfers by monitoring network packet data transfer volume.	See '338 claim 1 and associated discussion in my expert report. **103:** L.T. Heberlein, G.V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, D. Wolber., "A Network Security Monitor," Proc. 1990

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		Symposium on Research in Security and Privacy, pp. 296-304, May 1990 [SYM_P_0068974- SYM_P_0068956] (300) [SYM_P_0068978] Ji-Nao: Y. Frank Jou et al., "Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure," Technical Report CDRL A005, DARPA Order No. E296, Dept of Computer Science North Carolina State University, April 1997, posted on MCNC website at least as early as October 1997 [SYMP_P0070541 – SYM_P_0070582] NetRanger: NetRanger User's Guide 1.3.1. WheelGroup Corporation, 1997 [SYM_P_0074948 – SYM_P_0075282], 4-61, 4-63, 4-72 ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A.
5	The method of claim 1, wherein the measure monitors network connections by monitoring network connection requests.	See '338 claim 1 and associated discussion in my expert report. **103:** NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 1-10 [SYM_P_0074983], 4-63 [SYM_P_0075119], C-4 to C-5 [SYM_P_0075215-16], 4-62 [SYM_P_0075118]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A. synkill. *See* Schuba et al., "Analysis of a Denial of Service Attack on TCP," Proc. of the 1997 IEEE Symposium on Security and Privacy, Oakland, CA, 208-23 (May 4-7 1997) [SYM_P_0535408-28], 214-222 [SYM_P_0535419-27]. Network Security Probe. *See* P. Rolin, L. Toutain, and S. Gombault, "Network Security Probe," Proc. of the 2nd ACM Conference on Computer and Communications Security, 229-40 (ACM 1994) [SYM_P_0074513-24], 235-37 [SYM_P_0074519-21].

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		Gabriel. *See* Gabriel Man Page (1/9/1997) [SYM_P_0527549-52].
6	The method of claim 1, wherein the measure monitors network connections by monitoring network connection denials.	See '338 claim 1 and associated discussion in my expert report. **103:** NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-72 [SYM_P_0075128], 4-62 [SYM_P_0075118]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A.
7	The method of claim 1, wherein the measure monitors network connections by monitoring a correlation of network connections requests and network connection denials.	**103:** NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], [SYM_P_0074948-5282], 1-10 [SYM_P_0074983], 4-63 [SYM_P_0075119], C-4 to C-5 [SYM_P_0075215-16], 4-62 [SYM_P_0075118], 4-72 [SYM_P_0075128]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A.
8	The method of claim 1, wherein the measure monitors errors by monitoring error codes included in a network packet.	See '338 claim 1 **103:**

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-67 [SYM_P_0075123], 4-82 [SYM_P_0075138]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A. SNMP/RMON. *See* my expert report. Jeremy Frank, "Artificial Intelligence and Intrusion Detection: Current and Future Directions," Proc. of the 17th National Computer Security Conference (1994) [SYM_P_0073569-80]
10	The method of claim 8 wherein an error code comprises an error code indicating a reason a packet was rejected.	See '338 claim 1 and associated discussion in my expert report. **103:** NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-67 [SYM_P_0075123]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A. SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856]. SNMP/RMON. *See* my expert report.
11	The method of claim 1, further comprising responding based on the determining whether the	"In addition to domain surveillance, the domain monitor is responsible for reconfiguring system parameters, interfacing with other monitors beyond the domain, and reporting threats against the domain to administrators." p. 356 [SYM_P_0068834]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
	difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.	[See Fig. 1 label: RESOLVER (Countermeasure Unit)] "• **Decision Unit Configuration**: This refers to the semantics used by the resolver's decision unit for merging the analysis results from the various analysis engines. The semantics include the response criteria used by the decision unit for invoking countermeasure handlers. … • **Valid Response Methods**: Various response functions can be made available to the resolver as it receives intrusion reports from its analysis engines or intrusion summaries from subscribees. These are pre-programmed countermeasure methods that the resolver may invoke as intrusion summaries are received." p. 358 [SYM_P_0068836] "Implementation of the response policy, including coordinating the dissemination of the analysis results, is the responsibility of the EMERALD resolver. The resolver is an expert system that receives the intrusion and suspicion reports produced by the profiler and signature engines, and based on these reports invokes the various response handlers defined within the resource object. … In addition to its external-interface responsibilities, the resolver operates as a fully functional decision engine, capable of invoking real-time countermeasures in response to malicious or anomalous activity reports produced by the analysis engines. Countermeasures are defined in the response-methods field of the resource object. Included with each valid response method are evaluation metrics for determining the circumstances under which the method should be dispatched. These response criteria involve two evaluation metrics: a threshold metric that corresponds to the measure values and scores produced by the profiler engine, and severity metrics correspond to subsets of the associated attack sequences defined within the resource object. The resolver combines the metrics to formulate its monitor's response policy. Aggressive responses may include direct countermeasures such as closing connections or terminating processes. More passive responses may include the dispatching of integrity-checking handlers to verify the operating state of the analysis target." p. 360-61 [SYM_P_0068838- SYM_P_0068839]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		"EMERALD monitors incorporate a duplex messaging system that allows them to correlate activity summaries and countermeasure information in a distributed hierarchical analysis framework. …Once the subscription request is accepted by the server, the server module forwards events or analysis results to the client automatically as data becomes available, and may dynamically reconfigure itself as requested by the client's control requests." … Intermonitor communication also operates using the subscription-based hierarchy. A domain monitor subscribes to the analysis results produced by service monitors, and then propagates its own analytical results to its parent enterprise monitor. The enterprise monitor operates as a client to one or more domain monitors, allowing them to correlate and model enterprise-wide activity from the domain-layer results Domain monitors operate as servers to the enterprise monitors, and as clients to the service-layer monitors deployed throughout their local domain. This message scheme would operate identically if correlation were to continue at higher layers of abstraction beyond enterprise analysis." p. 361-62 [SYM_P_0068839- SYM_P_0068840] "Through the internal message system, the resolver submits configuration requests and probes to the analysis engines, and receives from the analysis engines their analysis results. The analysis engines operate as servers providing the resolver with intrusion or suspicion reports either asynchronously or upon request." p. 362 [SYM_P_0068840] "Domain monitors may also operate within an enterprise hierarchy, where they disseminate intrusion reports to enterprise monitors for global correlation. Where trust exists between domains, peer-to-peer subscription provides a useful technique for keeping domains sensitized to malicious activity occurring outside their view. Enterprise-layer monitors attempt to model and detect coordinated efforts to infiltrate domain perimeters or prevent interconnectivity between domains. Enterprise surveillance may be used where domains are interconnected under the control of a single organization, such as a large privately owned WAN. Enterprise surveillance is very similar to domain surveillance: the *enterprise monitor* subscribes to various domain monitors, just as the domain monitors subscribed to various local service monitors. The enterprise monitor (or monitors, as it would be important to avoid centralizing any analysis) focuses on network-wide threats

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		such as Internet worm-like attacks, attacks repeated against common network services across domains, or coordinated attacks from multiple domains against a single domain." p. 363 [SYM_P_0068841]
12	The method of claim 11, wherein responding comprises transmitting an event record to a network monitor.	See '338 claim 11 "Implementation of the response policy, including coordinating the dissemination of the analysis results, is the responsibility of the EMERALD resolver. The resolver is an expert system that receives the intrusion and suspicion reports produced by the profiler and signature engines, and based on these reports invokes the various response handlers defined within the resource object. ... EMERALD supports extensive intermonitor sharing of analysis results throughout its layered analysis architecture. Resolvers are able to request and receive intrusion reports from other resolvers at lower levels in the analysis hierarchy. ... This tiered collection and correlation of analysis results allows EMERALD monitors to represent and profile more global malicious or anomalous activity that is not visible from the local monitoring of individual network services and assets... For example, an intrusion report produced by a service monitor in one domain could be propagated to an enterprise monitor, which in turn sensitizes service monitors in other domains to the same activity." 360-61 [SYM_P_0068838- SYM_P_0068839] "Externally, EMERALD monitors interoperate with one another in a manner analogous to internal communication: service monitors produce local analysis results that are passed to the domain monitor; domain monitors correlate service monitor results, producing new results that are further propagated to enterprise monitors; enterprise monitors correlate and respond to the analysis results produced by domain monitors. ... A domain monitor subscribes to the analysis results produced by service monitors, and then propagates its own analytical results to its parent enterprise monitor. The enterprise monitor operates as a client to one or more domain monitors, allowing them to correlate and model enterprise-wide activity from the domain-layer results." 362 SYM_P_0068840]
13	The method of claim 12,	"Domain-wide analysis forms the second tier of EMERALD's layered network surveillance scheme. A *domain monitor* is

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
	wherein transmitting the event record to a network monitor comprises transmitting the event record to a hierarchically higher network monitor.	responsible for surveillance over all or part of the domain. *Domain monitors* correlate intrusion reports disseminated by individual service monitors, providing a domain-wide perspective of malicious activity (or patterns of activity). In addition to domain surveillance, the domain monitor is responsible for reconfiguring system parameters, interfacing with other monitors beyond the domain, and reporting threats against the domain to administrators. Lastly, EMERALD enables enterprise-wide analysis, providing a global abstraction of the cooperative community of domains. Enterprise-layer monitors correlate activity reports produced across the set of monitored domains. Enterprise-layer monitors focus on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, and coordinated attacks from multiple domains against a single domain. Through this correlation and sharing of analysis results, reports of problems found by one monitor may propagate to other monitors throughout the network." p. 356 [SYM_P_0068834] "Domain monitors may also operate within an enterprise hierarchy, where they disseminate intrusion reports to enterprise monitors for global correlation. Where trust exists between domains, peer-to-peer subscription provides a useful technique for keeping domains sensitized to malicious activity occurring outside their view. Enterprise-layer monitors attempt to model and detect coordinated efforts to infiltrate domain perimeters or prevent interconnectivity between domains. Enterprise surveillance may be used where domains are interconnected under the control of a single organization, such as a large privately owned WAN. Enterprise surveillance is very similar to domain surveillance: the *enterprise monitor* subscribes to various domain monitors, just as the domain monitors subscribed to various local service monitors. The enterprise monitor (or monitors, as it would be important to avoid centralizing any analysis) focuses on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, or coordinated attacks from multiple domains against a single domain." p. 363 [SYM_P_0068841]
14	The method of claim 13, wherein transmitting the event record to a network monitor	See '338 claim 13

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
	comprises transmitting the event record to a network monitor that receives event records from multiple network monitors.	
15	The method of claim 14, wherein the monitor that receives event records from multiple network monitors comprises a network monitor that correlates activity in the multiple network monitors based on the received event records.	See '338 claim 13
16	The method of claim 11, wherein responding comprises altering analysis of the network packets.	See '338 claim 11
17	The method of claim 11, wherein responding comprises severing a communication channel.	See '338 claim 11
18	The method of claim 1, wherein the network packets comprise TCP/IP packets.	*"The EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) environment is a distributed scalable tool suite for tracking malicious activity through and across large networks. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. It combines models from research in distributed high-volume event-correlation methodologies with over a decade of intrusion detection research and engineering experience. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable*

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		polymorphically at various abstract layers in a large network. These monitors contribute to a streamlined event-analysis system that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services on the Internet." p. 353 [SYM_P_0068831] "The typical target environment of the EMERALD project is a large enterprise network with thousands of users connected in a federation of independent administrative *domains*. Each administrative domain is viewed as a collection of local and network services that provide an interface for requests from individuals internal and external to the domain. Network services include features common to many network operating systems such as mail, HTTP, FTP, remote login, network file systems, finger, Kerberos, and SNMP. Some domains may share trust relationships with other domains (either peer-to-peer or hierarchical). Other domains may operate in complete mistrust of all others, providing outgoing connections only, or perhaps severely restricting incoming connections. Users may be local to a single domain or may possess accounts on multiple domains that allow them to freely establish connections throughout the enterprise." p. 354 [SYM_P_0068832]
19	The method of claim 1, wherein the network entity comprises a gateway, a router, or a proxy server.	"Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering." p. 355 [SYM_P_0068833] "Event Generation and Storage: Audit generation and storage has tended to be a centralized activity, and often gathers excessive amounts of information at inappropriate layers of abstraction. Centralized audit mechanisms place a heavy burden on the CPU and I/O throughput, and simply do not scale well with large user populations. In addition, it is difficult to extend centralized audit mechanisms to cover spatially distributed components such as network infrastructure (e.g., routers, filters, DNS, firewalls) or various common network services." p. 354 [SYM_P_0068832]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
21	A method of network surveillance, comprising:	See '338 claim 1
	monitoring network packets handled by a network entity;	See '338 claim 1
	building a long-term and multiple short-term statistical profiles of the network packets;	See '338 claim 1
	comparing one of the multiple short-term statistical profiles with the long-term statistical profile; and	See '338 claim 1
	determining whether the difference between the one of the multiple short-term statistical profiles and the long-term statistical profile indicates suspicious network activity.	See '338 claim 1
24	A computer program product, disposed on a computer readable medium, the product including instructions for causing a processor to:	See '338 claim 1
	receive network packets handled by a network entity;	See '338 claim 1
	build at least one long-term and at least one short-term statistical	See '338 claim 1

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
	profile from at least one measure of the network packets,	
	the measure monitoring data transfers, errors, or network connections;	See '338 claim 1
	compare at least one short-term and at least one long-term statistical profile; and	See '338 claim 1
	determine whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.	See '338 claim 1
25	A method of network surveillance, comprising:	See '338 claim 1
	receiving network packets at virtual private network entity; and	"The typical target environment of the EMERALD project is a large enterprise network with thousands of users connected in a federation of independent administrative *domains*. Each administrative domain is viewed as a collection of local and network services that provide an interface for requests from individuals internal and external to the domain. Network services include features common to many network operating systems such as mail, HTTP, FTP, remote login, network file systems, finger, Kerberos, and SNMP. Some domains may share trust relationships with other domains (either peer-to-peer or hierarchical). Other domains may operate in complete mistrust of all others, providing outgoing connections only, or perhaps severely restricting incoming connections. Users may be local to a single domain or may possess accounts on multiple domains that allow them to freely establish connections throughout the enterprise." p. 354 [SYM_P_0068832]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		"Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) ..." p. 355 [SYM_P_0068833] "It is at the transport layer where EMERALD addresses issues of communications security, integrity, and reliability. While it is important to facilitate interoperability among security mechanisms, this interoperability must be balanced with the need to ensure an overall level of operational integrity, reliability, and privacy. An essential element in the EMERALD messaging system design is the integration of secure transport to ensure a degree of internal security between EMERALD components and other cooperative analysis units." p. 362 [SYM_P_0068840] "For example, the intramonitor transport mechanisms may employ unnamed pipes [14], which provides a kernel-enforced private interprocess communication channel between the monitor components (this assumes a process hierarchy within the monitor architecture)." p. 362-63 [SYM_P_0068840] "To ensure the security and integrity of the message exchange, the external transport may employ public/private key authentication protocols and session key exchange. Using this same interface, third-party analysis tools may authenticate and exchange analysis results and configuration information with EMERALD monitors in a well-defined, secure manner." p. 362-63 [SYM_P_0068840-SYM_P_0068841] **103:** SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_000501-856], 2-5 to 2-10 [SUN_000549-54].

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'338 Claim number	Claim Term	EMERALD 1997 (printed publication)
		NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 1-13 to 1-14 [SYM_P_0074986-87], B-10 to B-17 [SYM_P_0075204-11]. U.S. Patent No. 5,825,891 (Levesque) Key Management for Network Communication 10/29/1997 [SYM_P_0069852-SYM_P_0069866]
	building at least one long-term and at least one short-term statistical profile based on the received packets and	See '338 claim 1
	comparing at least one long-term statistical profile with at least one short-term statistical profile to determine whether the packets indicate suspicious network activity.	See '338 claim 1

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	*"The EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) environment is a distributed scalable tool suite for tracking malicious activity through and across large networks. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. It combines models from research in distributed high-volume event-correlation methodologies with over a decade of intrusion detection research and engineering experience. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network. These monitors contribute to a streamlined event-analysis system that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services on the Internet."* p. 353 [SYM_P_0068831] "The typical target environment of the EMERALD project is a large enterprise network with thousands of users connected in a federation of independent administrative *domains*. Each administrative domain is viewed as a collection of local and network services that provide an interface for requests from individuals internal and external to the domain. p. 354 [SYM_P_0068832] "EMERALD introduces a hierarchically layered approach to network surveillance that includes *service analysis* covering the misuse of individual components and network services within the boundary of a single domain; *domain-wide analysis* covering misuse visible across multiple services and components; and *enterprise-wide analysis* covering coordinated misuse across multiple domains." p. 355 [SYM_P_0068833]
	deploying a plurality of network monitors in the enterprise network;	"The typical target environment of the EMERALD project is a large enterprise network with thousands of users connected in a federation of independent administrative *domains*. Each administrative domain is viewed as a collection of local and network services that provide an interface for requests from individuals internal and external to the domain. p. 354 [SYM_P_0068832]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
		"We introduce the concept of dynamically deployable, highly distributed, and independently tunable *service monitors*. Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering. This localized coverage of network services and domain infrastructure forms the lowest tier in EMERALD's layered network-monitoring scheme." p. 355 [SYM_P_0068833] "All EMERALD monitors (service, domain, and enterprise) are implemented using the same monitor code-base." p. 357 [SYM_P_0068835]
	detecting, by the network monitors, suspicious network activity	"EMERALD employs a building-block architectural strategy using independent distributed surveillance monitors that can analyze and respond to malicious activity on local targets, and can interoperate to form an analysis hierarchy. This layered analysis hierarchy provides a framework for the recognition of more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an entire network enterprise." p. 355 [SYM_P_0068833] "In general, a monitor may include additional analysis engines that may implement other forms of event analysis, or a monitor may consist of only a single resolver implementing a response policy based on intrusion summaries produced by other EMERALD monitors. ... Multiple analysis engines implementing different analysis methods may be employed to analyze a variety of event streams that pertain to the same analysis target. These analysis engines are intended to develop significantly lower volumes of abstract *intrusion* or *suspicion reports*. The profiler and signature engines receive large volumes of event logs specific to the analysis target, and produce smaller volumes of intrusion or suspicion reports that are then fed to their associated *resolver*." p. 356 [SYM_P_0068834]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
	based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};	"**Event Generation and Storage**: Audit generation and storage has tended to be a centralized activity, and often gathers excessive amounts of information at inappropriate layers of abstraction. Centralized audit mechanisms place a heavy burden on the CPU and I/O throughput, and simply do not scale well with large user populations. In addition, it is difficult to extend centralized audit mechanisms to cover spatially distributed components such as network infrastructure (e.g., routers, filters, DNS, firewalls) or various common network services." p. 354 [SYM_P_0068832] "Service monitors are dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces). Service monitors may interact with their environment passively (reading activity logs) or actively via probing to supplement normal event gathering." p. 355 [SYM_P_0068833] "The generic EMERALD monitor architecture is illustrated in Figure 1. The architecture is designed to enable the flexible introduction and deletion of analysis engines from the monitor boundary as necessary. In its dual-analysis configuration, an EMERALD monitor instantiation combines signature analysis with statistical profiling to provide complementary forms of analysis over the operation of network services and infrastructure. In general, a monitor may include additional analysis engines that may implement other forms of event analysis, or a monitor may consist of only a single resolver implementing a response policy based on intrusion summaries produced by other EMERALD monitors. Monitors also incorporate a versatile application programmers' interface that enhances their ability to interoperate with the analysis target, and with other third-party intrusion-detection tools. Underlying the deployment of an EMERALD monitor is the selection of a target-specific event stream. The event stream may be derived from a variety of sources including audit data, network datagrams, SNMP traffic, application logs, and analysis results from other intrusion-detection instrumentation. The event stream is parsed, filtered, and formatted by the target-specific event-collection methods provided within the resource object definition (see Section III-B). Event records are then forwarded to the monitor's analysis engine(s) for processing. EMERALD's *profiler engine* performs statistical profile-based anomaly detection given a generalized event stream of an analysis target

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
		(Section III-C). EMERALD's *signature engine* requires minimal state-management and employs a rule-coding scheme that breaks from traditional expert-system techniques to provide a more focused and distributed signature-analysis model (Section III-D). Multiple analysis engines implementing different analysis methods may be employed to analyze a variety of event streams that pertain to the same analysis target." p. 356 [SYM_P_0068834] "Similarly, the analysis engines are responsible for establishing and maintaining a communication link with a target event collection method (or event filter) and prompting the reconfiguration of the collection method's filtering semantics when necessary. Event collection methods provide analysis engines with target-specific event records upon which the statistical and signature analyses are performed." p. 362 [SYM_P_0068840] "EMERALD also provides a framework for recognizing more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an entire network enterprise. … It generalizes to network environments the Safeguard experience [2], which overcame profile explosion and scalability problems by locally profiling the activities of subsystems and commands rather than of individual users." p. 364 [SYM_P_0068842] "EMERALD also extends the statistical-profile model of NIDES, to analyze the operation of network services, network infrastructure, and activity reports from other EMERALD monitors. Various other efforts have considered one of the two types of analysis - signature-based (e.g., Porras [18] has used a state-transition approach; the U.C. Davis and Trident DIDS [4] addresses abstracted analysis for networking, but not scalability; the Network Security Monitor [7] seeks to analyze packet data rather than conventional audit trails; Purdue [5] seeks to use adaptive-agent technology) or profile-based. More recent work in UC Davis' GrIDS effort [24] employs *activity graphs* of network operations to search for traffic patterns that may indicate network-wide coordinated attacks." p. 364 [SYM_P_0068842]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
		See also discussion in my expert report. **103:** NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-79 - 4-80 [SYM_P_0075135-36], 4-61 [SYM_P_0075117], 4-67 [SYM_P_0075123], 4-69 [SYM_P_0075125], 4-82 [SYM_P_0075138]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A. SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856]. SNMP/RMON: see my expert report.
	generating, by the monitors, reports of said suspicious activity; and	"Information correlated by a service monitor can be disseminated to other EMERALD monitors through a *subscription*-based communication scheme. Subscription provides EMERALD's message system both a push and pull data exchange capability between monitor interoperation (see Section III-F). EMERALD client monitors are able to subscribe to receive the analysis results that are produced by server monitors. As a monitor produces analysis results, it is then able to disseminate these results asynchronously to its client subscribers. Through subscription, EMERALD monitors distributed throughout a large network are able to efficiently disseminate reports of malicious activity without requiring the overhead of synchronous polling." pp. 355-56 [SYM_P_0068833- SYM_P_0068834] "Multiple analysis engines implementing different analysis methods may be employed to analyze a variety of event streams that pertain to the same analysis target. These analysis engines are intended to develop significantly lower volumes of abstract *intrusion* or *suspicion reports*. The profiler and signature engines receive large volumes of event logs specific to the analysis target, and produce smaller volumes of intrusion or suspicion reports that are then fed to their associated *resolver*." p. 356 [SYM_P_0068834]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
		"Event records are defined based on the contents of the monitor's target event stream(s). Analysis result structures are used to package the findings produced by the analysis engine. Event records and analysis results are defined similarly to allow the eventual hierarchical processing of analysis results as event records by subscriber monitors." p. 358 [SYM_P_0068836] "Externally, EMERALD monitors interoperate with one another in a manner analogous to internal communication: service monitors produce local analysis results that are passed to the domain monitor; domain monitors correlate service monitor results, producing new results that are further propagated to enterprise monitors; enterprise monitors correlate and respond to the analysis results produced by domain monitors. ... Through the internal message system, the resolver submits configuration requests and probes to the analysis engines, and receives from the analysis engines their analysis results. The analysis engines operate as servers providing the resolver with intrusion or suspicion reports either asynchronously or upon request." p. 362 [SYM_P_0068840]
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	"Domain-wide analysis forms the second tier of EMERALD's layered network surveillance scheme. A *domain monitor* is responsible for surveillance over all or part of the domain. *Domain monitors* correlate intrusion reports disseminated by individual service monitors, providing a domain-wide perspective of malicious activity (or patterns of activity). In addition to domain surveillance, the domain monitor is responsible for reconfiguring system parameters, interfacing with other monitors beyond the domain, and reporting threats against the domain to administrators. Lastly, EMERALD enables enterprise-wide analysis, providing a global abstraction of the cooperative community of domains. Enterprise-layer monitors correlate activity reports produced across the set of monitored domains. Enterprise-layer monitors focus on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, and coordinated attacks from multiple domains against a single domain. Through this correlation and sharing of analysis results, reports of problems found by one monitor may propagate to other monitors throughout the network." p. 356 [SYM_P_0068834] "**Decision Unit Configuration**: This refers to the semantics used by the resolver's decision unit for merging the analysis results from the various analysis engines. The semantics include the response criteria used by the decision unit for invoking countermeasure

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
		handlers." p. 358 [SYM_P_0068836] "Implementation of the response policy, including coordinating the dissemination of the analysis results, is the responsibility of the EMERALD resolver. The resolver is an expert system that receives the intrusion and suspicion reports produced by the profiler and signature engines, and based on these reports invokes the various response handlers defined within the resource object. ... EMERALD supports extensive intermonitor sharing of analysis results throughout its layered analysis architecture. Resolvers are able to request and receive intrusion reports from other resolvers at lower layers in the analysis hierarchy. As analysis results are received from subscribees, they are forwarded via the monitor's event filters to the analysis engines. This tiered collection and correlation of analysis results allows EMERALD monitors to represent and profile more global malicious or anomalous activity that is not visible from the local monitoring of individual network services and assets (see Section IV). ... The resolver operates as the center of intramonitor communication. As the analysis engines build intrusion and suspicion reports, they propagate these reports to the resolver for further correlation, response, and dissemination to other EMERALD monitors. ... For example, an intrusion report produced by a service monitor in one domain could be propagated to an enterprise monitor, which in turn sensitizes service monitors in other domains to the same activity." p. 360-61 [SYM_P_0068838- SYM_P_0068839] "EMERALD monitors incorporate a duplex messaging system that allows them to correlate activity summaries and countermeasure information in a distributed hierarchical analysis framework. ...Once the subscription request is accepted by the server, the server module forwards events or analysis results to the client automatically as data becomes available, and may dynamically reconfigure itself as requested by the client's control requests." ... Intermonitor communication also operates using the subscription-based hierarchy. A domain monitor subscribes to the analysis results produced by service monitors, and then propagates its own analytical results to its parent enterprise monitor. The enterprise monitor

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
		operates as a client to one or more domain monitors, allowing them to correlate and model enterprise-wide activity from the domain-layer results. Domain monitors operate as servers to the enterprise monitors, and as clients to the service-layer monitors deployed throughout their local domain. This message scheme would operate identically if correlation were to continue at higher layers of abstraction beyond enterprise analysis." p. 361-62 [SYM_P_0068839- SYM_P_0068840] "Through the internal message system, the resolver submits configuration requests and probes to the analysis engines, and receives from the analysis engines their analysis results. The analysis engines operate as servers providing the resolver with intrusion or suspicion reports either asynchronously or upon request." p. 362 [SYM_P_0068840] "Domain monitors may also operate within an enterprise hierarchy, where they disseminate intrusion reports to enterprise monitors for global correlation. Where trust exists between domains, peer-to-peer subscription provides a useful technique for keeping domains sensitized to malicious activity occurring outside their view. Enterprise-layer monitors attempt to model and detect coordinated efforts to infiltrate domain perimeters or prevent interconnectivity between domains. Enterprise surveillance may be used where domains are interconnected under the control of a single organization, such as a large privately owned WAN. Enterprise surveillance is very similar to domain surveillance: the *enterprise monitor* subscribes to various domain monitors, just as the domain monitors subscribed to various local service monitors. The enterprise monitor (or monitors, as it would be important to avoid centralizing any analysis) focuses on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, or coordinated attacks from multiple domains against a single domain." p. 363 [SYM_P_0068841]
2	The method of claim 1, wherein integrating comprises correlating	"*Domain monitors* correlate intrusion reports disseminated by individual service monitors, providing a domain-wide perspective of malicious activity (or patterns of activity)." p. 356 [SYM_P_0068834]

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances "EMERALD 1997"

'203 Claim number	Claim Term	EMERALD 1997 (printed publication)
	intrusion reports reflecting underlying commonalities.	"Above the service layer, signature engines scan the aggregate of intrusion reports from service monitors in an attempt to detect more global coordinated attack scenarios or scenarios that exploit interdependencies among network services." p. 360 [SYM_P_0068838] "Domain monitors may also operate within an enterprise hierarchy, where they disseminate intrusion reports to enterprise monitors for global correlation. Where trust exists between domains, peer-to-peer subscription provides a useful technique for keeping domains sensitized to malicious activity occurring outside their view. Enterprise-layer monitors attempt to model and detect coordinated efforts to infiltrate domain perimeters or prevent interconnectivity between domains. ... The enterprise monitor (or monitors, as it would be important to avoid centralizing any analysis) focuses on network-wide threats such as Internet worm-like attacks, attacks repeated against common network services across domains, or coordinated attacks from multiple domains against a single domain. As an enterprise monitor recognizes commonalities in intrusion reports across domains (e.g., the spreading of a worm or a *mail* system attack repeated throughout the enterprise), its resolver can take steps to help domains counter the attack, and can also help sensitize other domains to such attacks before they are affected." p. 363 [SYM_P_0068841]
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	"In addition to domain surveillance, the domain monitor is responsible for reconfiguring system parameters, interfacing with other monitors beyond the domain, and reporting threats against the domain to administrators." p. 356 [SYM_P_0068834] [See Fig. 1 label: RESOLVER (Countermeasure Unit)] "• **Decision Unit Configuration**: This refers to the semantics used by the resolver's decision unit for merging the analysis results from the various analysis engines. The semantics include the response criteria used by the decision unit for invoking countermeasure